generating a secret key (p, q, s, β) consisting of elements p, q, s, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $s \in \mathbf{Z}$, $gh^3 \equiv 1 \pmod{pq}$,
- $\beta \in \mathbf{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}\,(p-1, q-1)}$,

and

generating a public key (n, g, h, k, l, α) consisting of elements n, g, h, k, l, and α (k is the bit length of pq) where:

- $\alpha, g, h, k, l \in Z$ $(0 < g, h < n)$,
- $n = p^d q$ (where d is an odd number);

(b) an encryption step which the sender conducts by working the sender-end device, according to a procedure comprising:

calculating the following equations with regard to a plaintext m $(0 < m < 2^{k-2})$ and a random number r $(0 \leqq r \leqq 1)$:

$C = m^{2\alpha} g^r \bmod n$, $D = h^r \bmod n$

calculating a Jacobi symbol $a = (m/n)$,

composing a ciphertext (C,D,a) from the obtained C,D and a, and

sending the ciphertext (C, D, a) to said receiver;

(c) a decryption step which said receiver conducts by working said receiver-end device according to a procedure comprising:

a

calculating the following from the ciphertext (C, D, a) using said secrete key (p, q, s, β) where:

$$m_{1,p} = (CD^{s})^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^{s})^{\frac{\beta(q+1)}{4}} \bmod q$$

and

finding one that fulfills conditions $(x/n) = a$ and $0 < x < 2^{k-2}$ from among $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ and determining the one as the plaintext m (where ϕ represents ring isomorphism mapping from $Z/(p) \times Z(q)$ to $Z/(pq)$ according to Chinese remainder theorem).

a1

3. (Amended) The public-key encryption method as recited in claim 2, further comprising:

a step that said sender composes said plaintext m including check data for verifying the recovery of true information.

---

7. (Amended) A public-key decryption method for decrypting a ciphertext encrypted in accordance with the method of claim 6, comprising the steps of:

a2

carrying out the decryption procedure in the public-key encryption method set forth in claim 2;

verifying the validity of the calculation procedure by

exclusive OR and data coherence executed as set forth in claim 6.

8. (Amended) A public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key, said public-key encryption method comprising:

(a) a key generation step which the receiver conducts by working the receiver-end device according to a procedure comprising:

generating a secret key (p, q, β) consisting of elements p, q, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $\beta \in \boldsymbol{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$,

and

generating a public key (n, k, α) consisting of elements n, k, and α (k is the bit length of pq), where:

- $\alpha, k \in \boldsymbol{Z}$,
- $n = p^d q$ (where d is an odd number);

(b) encryption which the sender conducts by working the sender-end device according to a procedure comprising:

calculating the following equation with regard to a plaintext m $(0 < m < 2^{k-2})$ where:

$m_1 = (m0^{k1} \oplus G(r)) || (r \oplus H(m0^{k1} \oplus G(r)))$ $(0 < m_1 < 2^{k-2})$ (where

$G: \{0, 1\}^{k0} \rightarrow \{0, 1\}^n$, $H: \{0, 1\}^n \rightarrow \{0, 1\}^{k0}$ are suitable random functions, subject to $k = n + k_0 + 2$),

calculating a Jacobi symbol $a = (m_1/n)$ and the following equation:

$C = m_1^{2\alpha} \bmod n$,

composing a ciphertext (C,D,a) from the obtained C,D and a, and

sending the ciphertext (C, a) to said receiver,

(c) a decryption step which said receiver conducts by working said receiver-end device according to a procedure comprising:

calculating the following from the ciphertext (C, a), using said secrete key (p, q, β) where:

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q$$

finding x that fulfills conditions $(x/n) = a$ and $0 < x < 2^{k-2}$ from among $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ and determining the x as m'_1 (where ϕ represents ring isomorphism mapping from $Z/(p) \times Z(q)$ to $Z/(pq)$ according to Chinese remainder theorem), and

calculating the following, assuming $m'_1 = s' || t'$ (where s' is upper n bits of m'_1 and t' is lower k_0 bits thereof):

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

(where $[a]^n$ and $[a]_n$ represent upper n bits and lower n bits of the a, respectively. An asterisk (*) as the result of decryption denotes that decryption is unsuccessful), thereby obtaining the result of decryption.

9. (Amended) A public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key, said public-key encryption method comprising:

a^2

(a) a key generation step which the receiver conducts by working the receiver-end device, according to a procedure comprising:

generating a secret key (p, q, s, β) consisting of elements p, q, s, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $s \in \mathbf{Z}$, $gh^3 \equiv 1 \pmod{pq}$,
- $\beta \in \mathbf{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}\,(p-1,\ q-1)}$,

and

generating a public key (n, g, h, k, l, α) consisting of elements n, g, h, k, l, and α (k is the bit length of pq) where:

- α, g, h, k, l $\in \mathbf{Z}$ $(0 < g, h < n)$,
- $n = p^d q$ (where d is an odd number);

(b) encryption which the sender conducts by working the sender-end device, according to a procedure comprising:

calculating the following equation with regard to a plaintext m $(0 < m < 2^{k-1})$ and a random number r' $(0 \leqq r' \leqq 1)$:

$m_1 = (m0^{k1} \oplus G\ (r))\ ||(r \oplus H\ (m0^{k1} \oplus G(r)))\quad (0 < m_1 < 2^{k-2})$

(where G: $\{0, 1\}^{k0} \rightarrow \{0, 1\}^n$, H: $\{0, 1\}^n \rightarrow \{0, 1\}^{k0}$ are suitable random functions, subject to $k = n + k_0 + 2$),

calculating a Jacobi symbol $a = (m_1/n)$ and the following equations:

$C = m_1^{2\alpha} g^{r'} \bmod n$, $D = h^{r'} \bmod n$,

Composing a ciphertext (C,D,a) from the obtained C,D and a, and

sending the ciphertext (C, D, a) to said receiver;

(c) decryption which said receiver conducts by working said receiver-end device, according to a procedure comprising:

calculating the following from the ciphertext (C, D, a),using said secrete key (p, q, s, β) where:

$C = m_1^{2\alpha} g^{r'} \bmod n$, $D = h^{r'} \bmod n$,

finding x that fulfills conditions $(x/n) = a$ and $0 < x < 2^{k-2}$ from among $\phi\ (m_{1,p}, m_{1,q})$, $\phi\ (-m_{1,p}, m_{1,q})$, $\phi\ (m_{1,p}, -m_{1,q})$, $\phi\ (-m_{1,p}, -m_{1,q})$ and determining the x as m'_1 (where ϕ represents ring isomorphism mapping from Z/(p) $\times$ Z (q) to Z/

(pq) according to Chinese remainder theorem), and

calculating the following, assuming $m'_1 = s'||t'$ (where s' is upper n bits of m'_1 and t' is lower k_0 bits thereof):

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases}$$

(where $[a]^n$ and $[a]_n$ represent upper n bits and lower n bits of the a, respectively. An asterisk (*) as the result of decryption denotes that decryption is unsuccessful), thereby obtaining the result of decryption.

a2

10. (Amended) A public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key, said public-key encryption method comprising:

(a) a key generation step which the receiver conducts by working the receiver-end device, according to a procedure comprising:

generating a secret key (p, q, s, β) consisting of elements p, q, s, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$;
- $s \in \boldsymbol{Z}$, $gh^3 \equiv 1 \pmod{pq}$,
- $\beta \in \boldsymbol{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}(p-1, q-1)}$,

and

generating a public key (n, g, h, k, l, α) consisting of elements n, g, h, k, l, and α (k is the bit length of pq) where:

- $\alpha, g, h, k, l \in Z$ $(0 < g, h < n)$,
- $n = p^d q$ (where d is an odd number),

(b) encryption which the sender conducts by working the sender-end device, according to a procedure comprising:

calculating the following equation with regard to a plaintext m $(0 < m < 2^n)$:

$m_1 = (m \oplus G(r)) \,||\, (r \oplus H(m \oplus G(r)))$ $(0 < m_1 < 2^{k-2})$

a^2

(where $G: \{0, 1\}^{k0} \rightarrow \{0, 1\}^n$, $H: \{0, 1\}^n \rightarrow \{0, 1\}^{k0}$ are suitable random functions, subject to $k = n + k_0 + 2$),

calculating a Jacobi symbol $a = (m_1/n)$ and the following equations:

$C = m_1^{2\alpha} g^{F(m1)} \bmod n$, $D = h^{F(m1)} \bmod n$

(where $F: \{0, 1\}^{n+k0} \rightarrow \{0, 1\}^l$ is a suitable random function),

composing a ciphertext (C,D,a) from the obtained C,D and a, and

sending the ciphertext (C, D, a) to said receiver;

(c) decryption which said receiver conducts by working said receiver-end device, according to a procedure comprising:

calculating the following from the ciphertext (C, D, a), using said secrete key (p, q, s, β) where:

$$m_{1,p} = (CD^{e})^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^{e})^{\frac{\beta(q+1)}{4}} \bmod q$$

finding x that fulfills conditions $(x/n) = a$ and $0 < x < 2^{k-2}$ from among $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ and determining the x as m'_1 (where ϕ represents ring isomorphism mapping from $Z/(p) \times Z(q)$ to $Z/(pq)$ according to Chinese remainder theorem), and

a^2

calculating the following, assuming $m'_1 = s' || t'$ (where s' is upper n bits of m'_1 and t' is lower k_0 bits thereof):

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases}$$

(where, C' and D' are obtained by:

$C' = m'^{2\alpha}_1 g^{F(m'1)} \bmod n$, $D' = h^{F(m'1)} \bmod n$

and $[a]^n$ and $[a]_n$ represent upper n bits and lower n bits of the a, respectively, wherein asterisk (*) as the result of decryption denotes that decryption is unsuccessful),

thereby obtaining the result of decryption.

---

12. (Amended) A public-key encryption method for data transmitted between a sender who encrypts data to send with a public key and a receiver who decrypts the data encrypted and delivered to the receiver with a secret key corresponding to said public key, said public-key encryption method comprising:

a^3

(a) a key generation step which the receiver conducts

by working the receiver-end device, according to a procedure comprising:

generating a secret key (p, q, s, β) consisting of elements p, q, s, and β, where:

- p and q are prime numbers, $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$,
- $s \in \mathbf{Z}$, $gh^3 \equiv 1 \pmod{pq}$,
- $\beta \in \mathbf{Z}$, $\alpha\beta \equiv 1 \pmod{\mathrm{lcm}\ (p-1, q-1)}$,

and

generating a public key $(n, g, h, k, 1, \alpha)$ consisting

a^3

of elements n, g, h, k, 1, and α (k is the bit length of pq) where:

- α, g, h, k, $1 \in Z$ $(0 < g, h < n)$,
- $n = p^d q$ (where d is an odd number);

(b) encryption which the sender conducts by working the sender-end device, according to a procedure comprising:

selecting a random number r $(0 < r < 2^{k0})$ with regard to a plaintext m $(0 < m < 2^n)$,

calculating the following:

$m_1 = m \,||\, r$

(where $F: \{0, 1\}^{n+k0} \rightarrow \{0, 1\}^1$ is a suitable random function, subject to $k = n + k_0 + 2$),

calculating a Jacobi symbol $a = (m_1/n)$ and the following equations:

$C = m_1^{2\alpha} g^{F(m1)} \bmod n$, $D = h^{F(m1)} \bmod n$,

Composing a ciphertext (C,D,a) from the obtained C,D

and a, and

sending the ciphertext (C, D, a) to said receiver;

(c) decryption which said receiver conducts by working said receiver-end device, according to a procedure comprising:

calculating the following from the ciphertext (C, D, a), using said secrete key (p, q, s, β):

$$m_{1,p} = (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p,$$
$$m_{1,q} = (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q$$

finding x that fulfills conditions (x/n) = a and 0 < x < 2^{k-2} from among $\phi(m_{1,p}, m_{1,q})$, $\phi(-m_{1,p}, m_{1,q})$, $\phi(m_{1,p}, -m_{1,q})$, $\phi(-m_{1,p}, -m_{1,q})$ and determining the x as m'_1 (where ϕ represents ring isomorphism mapping from Z/(p) $\times$ Z (q) to Z/(pq) according to Chinese remainder theorem), and

a3

calculating the following:

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases}$$

(where, C' and D' are obtained by:

$C' = m'^{2\alpha}_1 g^{F(m'1)} \bmod n$, $D' = h^{F(m'1)} \bmod n$

and $[a]^n$ and $[a]_n$ represent upper n bits and lower n bits of the a, respectively, wherein asterisk (*) as the result of decryption denotes that decryption is unsuccessful), thereby obtaining the result of decryption.